REMARKS

Claims 1, 3-7, 11-12, 16-17, 19-20, 22-26, 28, 30-31, 35-36, 38-39, 41-45, 47, 49-50, 54-55, 57-62, 64 and 67-70 are pending with claims 1, 20, and 39 being independent. Claims 68-70 are renumbered to claims 67-69 respectively to correct missed claim number 67. Claims 1, 16, 19, 20, 39, 58, 61-63, 64 and 68-70 are amended. A new claim 70 is added.

Claims 1, 3-7, 11-12, 16-17, 19-20, 22-26, 28, 30-31, 38-39, 41-45, 47, 49-50, 54-55, 57-62, 64 and 68-70 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Cox (U.S. 6,738,814) in view of Eichstaedt et al. (U.S. 6,662,230) and in further view of Maher, III et al. (U. S. 6,654,373), in further view of Alcendor (U. S. 6,337,899). Applicant has amended claims 1, 20, and 39 to obviate this rejection.

As amended, claim 1 recites a method for securing an accessible computer system, the method includes, receiving more than one data packet at a network device, each data packet including a payload portion and an attribute portion and being communicated between at least one access requestor and at least one access provider through the network device, monitoring at the network device at least the payload portion of the data packets directed from at least one of the access providers to at least one of the access requestors by scanning the payload portion for at least one predetermined pattern and counting a number of data packets having payload portions that include the predetermined pattern; and using the network device to deny subsequent data packets from the access requestor to the access provider at the when a number of payload portions of the data packets received from the access provider to the access requestor is deemed to include the predetermined pattern exceed a configurable threshold number.

Applicants respectfully request reconsideration and withdrawal of the rejection because Cox, Eichstaedt, Maher and Alcendor, either alone or combined as proposed, fail to disclose or suggest: i) monitoring at the network device at least the payload portion of the data packets directed from at least one of the access providers, and ii) using the network device to deny subsequent data packets from the access requestor to the access provider at the network device when a number of payload portions of the data packets received from the access provider to the

access requestor is deemed to include the predetermined pattern exceed a configurable threshold number, as recited in independent claim 1.

The Office Action agrees that the Cox fails to teach monitoring at least the payload portion of the data packets directed from at least one of the access providers and denying subsequent data packets from the access requestor to the access provider when a number of payload portions of the data packets received from the access provider to the access requestor include the predetermined pattern exceed a configurable threshold number. The office Action relies on Alcendor for the teaching of these features.

However, as amended, independent claim 1 further clarifies the features of i) monitoring at the network device at least the payload portion of the data packets directed from at least one of the access providers, ii) using the network device to deny subsequent data packets from the access requestor to the access provider when a number of payload portions of the data packets received from the access provider to the access requestor include the predetermined pattern exceed a configurable threshold number. Support for the newly clarified features is found throughout the disclosure, including the paragraphs that begin on lines 26 of page 3 to line 24 of page 6 of the specification, and Figures 1 and 2.

Alcendor does not block subsequent data packets from reaching the access provider via an intermediate network device. Rather, Alcendor deals with authentication of telephony response systems, in which each inbound call is sent to the access provider for consideration such that a decision on a presently evaluated packet is not used to deny access to a subsequent data packet. More specifically, as shown in paragraph 2-3 of column 7 and Fig. 4 of Alcendor, when a user's authentication fails (407) and when the user also fails a limited number of retries (405), the user is then redirected to reselect a desired service (401), which would again lead the user to be authenticated. (403 and 407). Thus, the same user could try over and over to submit bad passwords, never fully being blocked. Thus Alcendor is incapable of ii) "denying subsequent data packets from the access requestor to the access provider at the network device ..." as recited in claim 1. At most, Alcendor merely teaches temporarily inconveniencing the user by making them reselect the desired service. By contrast, Applicant actually blocks the user from submitting subsequent data packets to the access provider by the use of the network device.

This distinction is particularly significant since its absence from the Alcendor's patent makes Alcendor's teaching incapable of addressing denial of service attacks, which are specifically addressed by the Applicant as one potential application of the instant technology. For example, by using a separate network device to monitor and control data packets before the access provider, Applicant may be able to save the access provider from having to evaluate subsequently incoming data packets otherwise received from denial of service attackers, a feature that is not accomplished by Alcendor.

Therefore, Alcendor's patent, like Cox, Eichstaedt and Mahet, fails to teach or suggest the features of i) monitoring at the network device at least the payload portion of the data packets directed from at least one of the access providers, ii) using the network device to deny subsequent data packets from the access requestor to the access provider at the network device when a number of payload portions of the data packets received from the access provider to the access requestor are deemed to include the predetermined pattern exceed a configurable threshold number. Thus Alcendor's patent cannot be properly combined with the other references to suggest such features.

For at least these reasons, the proposed combination of Cox, Eichstaedt, Maher and Alcendor fail to teach or suggest the features of i) monitoring at the network device at least the payload portion of the data packets directed from at least one of the access providers, ii) using the network device to deny subsequent data packets from the access requestor to the access provider at the network device when a number of payload portions of the data packets received from the access provider to the access requestor are deemed to include the predetermined pattern exceed a configurable threshold number.

Moreover, the proposed combination is not proper. As indicated earlier, Alcendor's patent does not focus on denial of service attacks. Because of this lack of focus, it would not be obvious to modify the teachings of the other cited references based on the teachings of this reference.

The Office Action's statement of motivation also is deficient. Page 5 of the office action indicates that "At the time of the invention was made, one of ordinary skill in the art would have been motivated to monitor and limit data packets directed from the access provider to the access

requestor in order to limit the amount of access in the system, therefore enhancing its security." This statement of motivation is premised on the desirability of obtaining a feature that is missing from both the claims and the references. It suggests the desirability of "limiting data packets directed from the access provider to the access requestor in order to limit the amount of access in the system." Applicant's claims do not require a limitation of packets directed from the access provider to the access requestor. Alcendor's patent is similarly deficient in disclosing such.

For at least these reasons, independent claim 1 and its dependant claims are believed to be allowable over the applied combination of references.

Similarly, independent claim 20 recites "..to deny communication of subsequent data packets from the access requestor to the access provider when a number of payload portions of data packets received from the access provider to the access requestor that include the predetermined pattern exceed a configurable threshold number."

Independent claim 39 recites "...to deny communication of subsequent access by data packets from the access requestor to the access provider when a number of payload portions of the data packets received from the access provider to the access requestor that include the predetermined pattern exceed a configurable threshold number."

For at least the similar reasons as stated above, independent claim 20, 39 and their respective dependant claims are believed to be allowable over the applied combination of references.

It is believed that all claims are in condition for allowance, and such action is respectfully requested to the Examiner.

Please apply any charges or credits to deposit account 06-1050.

Respectfully submitted,

Date: 5/3/2006

W. Karl Renner
Reg. No. 41,265

Fish & Richardson P.C.
1425 K Street, N.W.
11th Floor
Washington, DC 20005-3500
Telephone: (202) 783-5070
Facsimile: (202) 783-2331

40326161.doc